Warszawa, 28 stycznia 2019 r.

Prezes Urzędu Ochrony Danych Osobowych

ul. Stawki 2

00-193 Warszawa

Skarżąca: Katarzyna Szymielewicz

adres zamieszkania:

adres do korespondencji: ul. Orzechowska 4/4, 02-068 Warszawa

reprezentowana przez

Fundację Panoptykon

KRS: 0000327613

ul. Orzechowska 4/4, 02-068 Warszawa

administrator danych:

Interactive Advertising Bureau Europe A.I.S.B.L. z siedzibą w Belgii (11 Rond-Point Schuman, 1040 Bruksela).

SKARGA
NA NIEZGODNE Z PRAWEM PRZETWARZANIE DANYCH OSOBOWYCH

Niniejszym, na podstawie art. 61 ustawy z 10 maja 2018 r. o ochronie danych osobowych w zw. z art. 80 i art. 77 Rozporządzenia Parlamentu i Rady (UE) nr 2016/679 – ogólne rozporządzenie o ochronie danych osobowych (**dalej: RODO**), działając w imieniu Katarzyny Szymielewicz **(dalej: Skarżąca)** (umocowanie stanowi **Załącznik nr 1** do pisma), Fundacja Panoptykon:

1. składa skargę na niezgodne z przepisami RODO przetwarzanie danych osobowych przez **Interactive Advertising Bureau Europe A.I.S.B.L.** z siedzibą w Belgii (11 Rond-Point Schuman, 1040 Bruksela). Podmiot ten przetwarza dane Skarżącej z naruszeniem przepisów art. 5, 6, 9, 12, 13, 24 i 25 RODO (szczegółowy opis stanu faktycznego i naruszeń znajduje się w uzasadnieniu).

2. wnosi o nakazanie Administratorowi, zgodnie z art. 58 ust. 2 lit. d) RODO, dostosowania operacji przetwarzania do przepisów RODO;

dodatkowo wnosimy o rozważenie:

3. podjęcia współpracy z organami nadzorczymi z innych państw członkowskich w trybie przewidzianym w art. 62 RODO
4. zastosowania, zgodnie z art. 58 ust. 2 lit. i) RODO, administracyjnej kary pieniężnej.

UZASADNIENIE

I. Wprowadzenie

1. Fundacja Panoptykon jest organizacją pozarządową, której działalność nie ma charakteru zarobkowego. Fundacja posiada siedzibę w Warszawie przy ul. Orzechowskiej 4/4 oraz wpisana jest do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz publicznych zakładów opieki zdrowotnej i do rejestru przedsiębiorców prowadzonych przez Sąd Rejonowy dla m.st. Warszawy, Wydział XII Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000327613. Cele statutowe Fundacji leżą w interesie publicznym i dotyczą m.in. działań w dziedzinie praw i wolności osób, których dane dotyczą. Odpis aktualny KRS stanowi **Załącznik nr 2**, a Statut Fundacji stanowi **Załącznik nr 3**. Fundacja Panoptykon reprezentuje p. Katarzynę Szymielewicz na podstawie umocowania udzielonego na podstawie art. 80 ust. 1 RODO udzielonego w dniu 25 stycznia 2019 r.
2. Niniejsza skarga (**dalej: Skarga**) dotyczy funkcjonowania rynku reklamy behawioralnej i związanych z nim naruszeń: artykułu 5, 6, 9, 12, 13, 24 i 25 RODO.
3. Naruszenia przepisów mają charakter masowy i dotyczą nie tylko Skarżącej, ale większości użytkowników Internetu. Z tego powodu wnosimy o rozpatrzenie niniejszej Skargi w kontekście szerokiej skali naruszeń, a także o podjęcie systemowych działań zmierzających do zapewnienia ochrony użytkowników Internetu przed naruszeniami reżimu ochrony danych przez Interactive Advertising Bureau – IAB jako jeden z dwóch (obok Google'a) podmiotów decydujących o kształcie i sposobie funkcjonowania rynku.
4. Jednocześnie zwracamy uwagę Prezesa na to, że analogiczna skarga została złożona w imieniu p. Szymielewicz na Google Ireland Ltd. – drugi podmiot, który dyktuje warunki na rynku reklamy behawioralnej poprzez strukturę o nazwie Authorized Buyers. Ze względu na podobieństwo zgłaszanych zastrzeżeń i systemowy charakter problemu uważamy za zasadne rozpatrzenie obu skarg wspólnie.
5. W odniesieniu do pkt. 3 petitum Skargi, wnosimy o **dołączenie do irlandzkiego i brytyjskiego dochodzenia przeciwko temu podmiotowi w trybie art. 62 RODO**. Sygnatura postępowania przed Data Protection Commissioner w Irlandii to: C-18-10-91, z kolei postępowanie przed ICO w Wielkiej Brytanii prowadzone jest pod sygnaturą:

RFA0785480. Zgodnie z informacjami otrzymanymi od irlandzkiego DPC, sprawa została podniesiona również na forum Europejskiej Rady Ochrony Danych. Postępowania te zostały zapoczątkowane przez wystąpienia i skargi dra Johnny'ego Ryana, Chief Policy Officer w firmie Brave, Jima Killocka, Dyrektora Wykonawczego brytyjskiej organizacji Open Rights Group i Michaela Veale'a z University College London. Treść wystąpień w języku angielskim stanowi **Załącznik nr 4**.

6. Dodatkowo, 8 listopada 2018 r. Fundacja Panoptykon, wspólnie z brytyjską organizacją Privacy International wystąpiła do Prezesa Urzędu Ochrony Danych Osobowych o podjęcie działań wobec podmiotów zajmujących się odsprzedażą danych na rynku reklamy behawioralnej (tzw. brokerów danych). W piśmie z 10 stycznia 2019 r. Urząd poinformował nas o swoich działaniach. Sprawa została opatrzona sygnaturą ZSPR.027.354.2018.LS.I.26281 (odpowiedź Prezesa UODO na wystąpienie stanowi **Załącznik nr 5**).

II. Kluczowe problemy

7. Fundamenty rynku reklamy behawioralnej tworzą dwa główne systemy, które funkcjonują w tzw. modelu *real-time bidding* (*RTB*, w wolnym tłumaczeniu: licytacja w czasie rzeczywistym):
   a. **„OpenRTB"** – stworzony przez IAB system powszechnie wykorzystywany w branży mediów i reklamy;
   b. **„Authorized Buyers"** – własnościowy system RTB Google'a funkcjonujący równolegle do OpenRTB, nazwa ta zastąpiła system znany dotychczas pod nazwą „DoubleClick Ad Exchange".
8. Niniejsza skarga dotyczy systemu Open RTB (**dalej: System**), którego autorem jest IAB. Systemu Authorized Buyers, z uwagi na innego administratora, dotyczy oddzielna skarga p. Szymielewicz.
9. **Celem Systemu jest wyświetlanie użytkownikom spersonalizowanej reklamy na portalach internetowych w drodze licytacji na giełdzie reklam.**
10. Przedmiotem licytacji na giełdzie reklam jest tzw. **impresja**, czyli pojedyncze wyświetlenie spersonalizowanej reklamy konkretnemu użytkownikowi w konkretnym miejscu. W licytacji na giełdzie reklam uczestniczą dwie grupy podmiotów: platformy podaży (*Supply-Side Platform, SSP*), których zadaniem jest – na zlecenie wydawców (portali internetowych) – wystawić dostępną impresję na sprzedaż, oraz platformy popytu (*Demand-Side Platform, DSP*), działające na zlecenie reklamodawców, których zadaniem jest składanie ofert w licytacji i zakup impresji. W komunikacji pomiędzy tymi platformami pośredniczy giełda reklam – jej zadania polegają na przyjęciu zgłoszenia (tzw. *bid request)* od platformy SSP, rozesłaniu go do współpracujących z nią platform DSP, przyjmowaniu ofert w licytacji i wyborze zwycięzcy.
11. **Cały wyżej opisany proces odbywa się w pełni automatycznie (w tzw. modelu *programmatic*) i jednorazowo angażuje nawet setki podmiotów.** *Bid request*, czyli zapytanie wysyłane przez platformę SSP na giełdę reklam i rozpowszechniane następnie

do platform DSP, zawiera liczne dane o użytkowniku: identyfikator użytkownika, tzw. *full referral URL* (zob. pkt poniżej) oraz wszelkie inne dane, które posiada platforma SSP: rok urodzenia, płeć, zainteresowania, lokalizacja, numer IP i inne.

12. *Full referral URL* zawiera link do strony, na której załadowanie czeka użytkownik oraz treść wyszukiwania lub adres, z którego użytkownik trafił na stronę. Tym informacjom towarzyszy nadana przez wydawcę kategoria strony, określona w oparciu o ustandaryzowany katalog (taksonomię) stworzony przez IAB na potrzeby Systemu. Kategoria nadana stronie może ujawniać bardzo wrażliwe dane o użytkowniku. Niektóre z kilkuset kategorii stworzonych przez IAB to: pomoc ofiarom przemocy, ciąża, problemy ze snem, uzależnienia, choroba dwubiegunowa, depresja itd. Szersza lista kategorii stosowana przez IAB jest częścią raportu technicznego stanowiącego **Załącznik nr 6**.
13. Dokładny opis technicznych aspektów funkcjonowania Systemu stanowi **Załącznik nr 6** (zawierający tzw. *Ryan Report* – anglojęzyczny raport przygotowany przez dra Johnny'ego Ryana na potrzeby postępowania przed irlandzkim i brytyjskim organem nadzorczym, ze wstępem Fundacji Panoptykon).
14. W naszej opinii z funkcjonowaniem Systemu związane są **trzy kluczowe problemy**:
    a. Po pierwsze, branża, której pierwotnym celem było świadczenie usług doboru spersonalizowanej reklamy, przerodziła się w **system masowego rozpowszechniania danych** oparty na:
        i. gromadzeniu szerokiego zakresu danych o jednostkach, znacznie przekraczającego zakres danych wymaganych do dopasowania reklamy;
        ii. przekazywaniu tych danych ogromnej liczbie podmiotów trzecich, które następnie wykorzystują dane w celach wykraczających poza te, które podmiot danych jest w stanie w pełni zrozumieć i w stosunku do których jest on w stanie wyrazić zgodę lub sprzeciw.

    W naszej opinii to wszechobecne i ingerujące w prywatność profilowanie użytkowników i rozpowszechnianie danych, odbywa się z naruszeniem przepisów RODO.

    b. Po drugie, System **uniemożliwia kontrolę dalszego rozpowszechniania udostępniania danych osobowych po tym, jak dane zostaną rozpowszechnione po raz pierwszy**. Sama liczba odbiorców danych powoduje, że podmiot rozpowszechniający dane (tj. wydawca za pośrednictwem platformy SSP) nie jest w stanie zapobiec nieautoryzowanemu dalszemu przetwarzaniu danych, ani prawidłowo poinformować podmiotów danych o wszystkich odbiorcach. Dane przekazywane są do wielu podmiotów, których celem jest łączenie danych z różnych źródeł i w konsekwencji tworzenie szczegółowych profili jednostek bez ich wiedzy i zgody. IAB ułatwia tę praktykę i nie przewiduje odpowiednich gwarancji mających na celu zapewnienie integralności i poufności danych. Sam sposób zaprojektowania Systemu i przyjęte środki techniczne i organizacyjne pokazują, że **naruszenia prywatności są immanentnie wpisane w jego funkcjonowanie**, naruszając tym samym przewidzianą w RODO zasadę *privacy by design*.

Dodatkowo, osoby, których dane dotyczą, zazwyczaj **nie wiedzą, czy i do kogo ich dane zostały przekazane** – ze względu na trudności z identyfikacją właściwych firm, jak i identyfikatorów użytkowników, którymi się posługują, realizacja prawa dostępu do danych jest w praktyce niemożliwa. Nie wiadomo również, czy podmioty te w ogóle stworzyły procedury, których celem jest ułatwienie realizacji praw przez osoby, których dane dotyczą.

c. Po trzecie, **rozpowszechniane dane mogą zawierać dane szczególnie chronione**. Jak wspominamy wyżej, *bid request* zawiera m.in. link strony, na której użytkownik czeka na wyświetlenie reklamy oraz jej kategorię. Jak pokazuje przywołane przez nas przykładowe kategorie, strony przeglądane przez użytkowników mogą wskazywać na ich orientację seksualną, pochodzenie etniczne, poglądy polityczne itd. Te dane mogą być dostępne bezpośrednio lub zostać w łatwy i skuteczny sposób wywnioskowane za pomocą współczesnych technik analitycznych. Prędkość, z jaką następuje licytacja na giełdzie reklam (ok. 200 ms) powoduje, że dane wrażliwe są rozpowszechniane bez zgody użytkownika oraz poza jakąkolwiek kontrolą (również poza kontrolą podmiotu rozpowszechniającego dane).

III. Standardy i procedury

15. Branża reklamy internetowej powołała organizację branżową – Interactive Advertising Bureau (IAB) – której zadaniem jest ustalanie standardów technicznych i organizacyjnych dla firm działających na rynku. Europejski oddział IAB – IAB Europe, przygotował standardy i procedury, które mają zastosowanie na europejskim rynku reklamy behawioralnej.

16. IAB Europe stworzyło dokument o nazwie „Europe Transparency & Consent Framework"[1] (dalej: **Standard IAB**). Standard IAB opiera się na założeniu, że użytkownik wyraża jedną, globalną zgodę na wszystkie przypadki rozpowszechniania danych do podmiotów trzecich podczas licytacji na giełdzie reklam.

17. W ten system wpisane jest fundamentalne ryzyko. Standard IAB wprost przewiduje, że w momencie, gdy dane jednostki zostaną rozpowszechnione, administrator danych **traci jakąkolwiek kontrolę nad tym, jak dane zostaną następnie wykorzystane**. Standard IAB przewiduje, że nawet w sytuacji, gdy odbiorca danych działa niezgodnie z prawem, dane mogą dalej być mu przekazywane[2]. W związku z utratą kontroli nad danymi przez administratora, jednostka również traci możliwość ustalenia, w jaki sposób jej dane są dalej wykorzystywane, choćby przez brokerów danych.

18. Dane rozpowszechniane są do firm licytujących na giełdzie reklam na zlecenie reklamodawców (platformom DSP) oraz brokerom danych. **Podmioty te mogą**

[1] http://www.iabeurope.eu/tcfdocuments/documents/legal/currenttcfpolicyFINAL.pdf.

[2] Por. fragment Standardu IAB, który pozwala podmiotowi rozpowszechniającemu dane kontynuować rozpowszechnianie danych do podmiotu trzeciego, który zgodnie z jego wiedzą narusza prawo: *If a CMP reasonably believes that a Vendor is not in compliance with the Specitfication, the Policies, or the law, it must promptly file a report with the MO accoring to MO procedures and **may**, as provided for by MO procedures, pause working with a Vendor while the matter is addressed.*

wykorzystywać dane w dowolny sposób, bez wiedzy i poza kontrolą użytkownika. Dane mogą być wykorzystane chociażby do połączenia ich z danymi o użytkowniku pochodzącymi z innych źródeł lub do profilowania użytkownika. To, do jakiego celu dane zostaną ostatecznie wykorzystane, może wykroczyć poza cele wskazane przez portal internetowy (wydawcę) – jedyny podmiot, z którym użytkownik wszedł w bezpośrednią interakcję. Wydawca, tracąc kontrolę nad danymi po ich rozpowszechnieniu na giełdzie reklam, nie ma możliwości wskazać wszystkich potencjalnych celów wykorzystania danych, które – jeśli użytkownik posiadłby o nich wiedzę – mogłyby się okazać niepokojące i niepożądane.

19. Ponadto, jak wskazywaliśmy wyżej, dane przekazywane setkom podmiotów uczestniczących w licytacji na giełdzie reklam, mogą zawierać dane szczególnie chronione. Brak jakiejkolwiek kontroli nad przekazywaniem tych danych stanowi poważny problem.

20. Standard IAB stanowi: *a Vendor must not transmit data to another Vendor without a <u>justified basis for relying on that Vendor's having a legal basis for processing the personal data</u>.*

    A zatem, uznaniu podmiotu rozpowszechniającego dane pozostawiono ustalenie, czy podmiot trzeci ma podstawę prawną do przetwarzania danych. W rezultacie preferencje samego użytkownika mogą nie zostać wzięte pod uwagę. To podmiot rozpowszechniający dane samodzielnie ocenia – na podstawie nieprecyzyjnych kryteriów – czy ma bliżej niezdefiniowane „uzasadnione podstawy", aby uważać, że podmiot trzeci posiada podstawę prawną do przetwarzania danych i tym samym przekazać mu dane.

21. Podsumowując, **Standard IAB ułatwia rozpowszechnianie danych osobowych do ogromnej liczby podmiotów trzecich, bez jednoczesnego zagwarantowania użytkownikom kontroli nad wykorzystywaniem danych**.

IV. Rola IAB na rynku reklamy behawioralnej

22. <u>Przetwarzanie danych osobowych</u>

    a. Zgodnie z art. 4 RODO, za dane osobowe uważa się informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Do kategorii danych osobowych należy także identyfikator internetowy w sytuacji, w której pozwala zidentyfikować jednostkę, bezpośrednio lub pośrednio (tzw. koncepcja *single out*[3]).

    b. Podstawowym identyfikatorem użytkownika w Internecie jest plik cookie, jednak coraz częściej do śledzenia użytkowników wykorzystywany jest także tzw. odcisk palca przeglądarki (*browser fingerprint*).

    c. W modelu RTB dane osobowe użytkowników są przetwarzane i rozpowszechniane nie tylko w postaci internetowych identyfikatorów, takich

[3] Por. opinię Grupy Roboczej Art. 29 w sprawie definicji danych osobowych, WP 136.

jak pliki *cookie*, ale również w postaci numeru IP[4], a także bardziej szczegółowych danych, takich jak link do strony, na której użytkownik czeka na wyświetlenie reklamy oraz treść wyszukiwania lub link, z których użytkownik trafił na tę stronę, kategoria nadana stronie (może ujawniać dane wrażliwe, np. kategoria „uzależnienia"), lokalizacja, rok urodzenia czy zainteresowania użytkownika[5].

23. <u>IAB jako administrator danych</u>

a. Biorąc pod uwagę definicję administratora danych jako podmiotu, który ustala cele i sposoby przetwarzania danych, orzecznictwo Trybunału Sprawiedliwości UE, które opowiada się za szeroką interpretacją tego pojęcia[6] oraz opinie Grupy Roboczej Art. 29[7], **uważamy, że IAB znajduje się w pozycji administratora danych osobowych**.

b. IAB to jeden z dwóch (obok Google) wiodących aktorów na rynku reklamy behawioralnej, który **organizuje, koordynuje i rozwija rynek** poprzez tworzenie specyfikacji API (interfejsu programistycznego) wykorzystywanego przez firmy uczestniczące w licytacjach na giełdach reklam (System). Specyfikacjom towarzyszą zasady ich stosowania: omówiony wyżej Standard IAB.

c. IAB posiada pełną kontrolę nad tym, jak zaprojektowany jest i jak działa rynek reklamy behawioralnej funkcjonujący w ramach Systemu, a więc **samodzielnie decyduje o tym, w jaki sposób przetwarzane będą dane osobowe**, np. przez określanie jakie elementy musi zawierać tzw. *bid request*, czyli zapytanie o składanie ofert na giełdzie reklam.

d. **Fakt, że IAB nie ma bezpośredniego dostępu do danych jest nieistotny.** W wyroku w sprawie Jehovan todistajat[8], Trybunał Sprawiedliwości UE orzekł, że wspólnota religijna świadków Jehowy, gromadząca informacje o swoich członkach (w odróżnieniu od informacji o osobach odwiedzanych przez członków), poprzez tworzenie wytycznych i map staje się współadministratorem danych osób odwiedzanych przez swoich członków, mimo że nie wchodzi z nimi w bezpośrednią interakcję i nie ma dostępu do tych danych.

e. Ten przypadek można wprost porównać do IAB, ponieważ jego rolą również jest **dostarczenie wytycznych i specyfikacji firmom uczestniczącym w licytacjach na giełdach reklam**. IAB posiada, tak jak wspólnota będąca przedmiotem analizy TSUE, ogólną wiedzę o tym, że przetwarzanie danych ma

---

[4] Trybunał Sprawiedliwości UE potwierdził, że adres IP może stanowić daną osobową, por. wyrok w sprawie Breyer, C-582/14.

[5] Por. techniczny opis „bid request" w Załączniku nr 2.

[6] Por. wyrok w sprawie Jehovan todistajat, C-25/17, par. 21 oraz wyrok w sprawie Wirtschaftsakademie, C-210/16.

[7] W opinii 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169) Grupa Robocza Art. 29 wskazała, że jeden ze sposobów ustalenia, czy dany podmiot jest administratorem, tj. ocena w oparciu o faktyczny wpływ tego pomiotu na przetwarzanie danych, może być szczególnie przydatny „w skomplikowanych środowiskach, korzystających często z nowych technologii informacyjnych, w których odpowiednie podmioty są często skłonne postrzegać się jako „pośrednicy", a nie jako odpowiedzialni administratorzy danych".

[8] C-25/17, *op.cit.*

miejsce i zna jego cel (dopasowanie reklamy w modelu RTB) oraz organizuje i koordynuje działalność swoich członków poprzez zarządzanie Systemem[9].

f. Argument, że stworzony przez IAB System to jedynie techniczny protokół, który nie nakazuje poszczególnym firmom przetwarzać danych, jest nietrafiony i niezgodny z prawdą. System umożliwia i ułatwia przetwarzanie i rozpowszechnianie danych, z uwagi na to, że związane z nim protokoły zawierają pola **zaprojektowane** tak, aby dochodziło do przekazywania danych, w tym danych wrażliwych (por. Załącznik nr 6).

24. Przetwarzanie danych osobowych Skarżącej

a. Skarżąca nie znajduje się w bezpośrednim stosunku z IAB.

b. W świetle powyższych uwag dotyczących funkcjonowania Systemu, roli IAB jako administratora danych na rynku reklamy behawioralnej i zarzutów naruszeń RODO opisanych poniżej, chcemy jednak zauważyć, że **istotą funkcjonowania Systemu jest to, że podmiot danych, w tym Skarżąca, nie ma wiedzy o tym, jakie dokładnie dane osobowe na jej temat są przetwarzane, przez jakie podmioty, w jakich celach i jak długo**. Skarżąca nie jest w stanie podać dokładnego zakresu danych osobowych, których administratorem jest IAB, ani dokładnego zakresu procesów przetwarzania właśnie z tego powodu, że podmiot ten nie poinformował Skarżącej, jakie dane i przez jakie podmioty będą przetwarzane.

c. Powyższe uwagi i raport stanowiący Załącznik nr 6 mają na celu wykazanie, że skala transakcji w modelu RTB jest ogromna. Licytacje w modelu RTB odbywają się w sposób ciągły, na niemalże każdej stronie internetowej odwiedzanej przed użytkownika. Dane osobowe są zatem rozpowszechniane w ramach Systemów RTB z wysoką częstotliwością i z dużą prędkością. Raport wskazuje również, jakie dane rozpowszechniane są w ramach Systemu. **Biorąc pod uwagę powszechność wykorzystywania Systemu, regularne rozpowszechnianie również danych osobowych Skarżącej jest nieuniknione.**

V. Problemy prawne związane z Systemem

25. Zarysowane powyżej tło ekosystemu reklamy behawioralnej pokazuje, że przetwarzanie danych wiąże się z wysokim ryzykiem naruszenia ochrony danych Skarżącej, w szczególności art. 5, 6, 9, 12, 13, 24 i 25 RODO.

26. W naszej opinii kwestią, która zasługuje na szczególne zbadanie, jest zgodność z przepisami Systemu i regulującym go Standardzie IAB. Poniżej opisujemy nasze główne zastrzeżenia w świetle zasad wynikających z RODO.

27. *Zgodność z prawem, rzetelność i przejrzystość przetwarzania danych*

[9] Por. pkt 71 wyroku: „Ponadto wspólnota świadków Jehowy **nie tylko ma, ogólnie rzecz biorąc, wiedzę na temat tego, że takie przetwarzanie odbywa się dla celów** propagowania jej wiary, lecz także **organizuje i koordynuje działalność kaznodziejską swoich członków**, w szczególności poprzez podział obszarów aktywności pomiędzy poszczególnych głosicieli”.

a. Z przewidzianych w art. 6 RODO podstaw prawnych do przetwarzania danych na rynku reklamy behawioralnej zastosowanie mogą mieć dwie: zgoda lub uzasadniony interes.

b. **Oparcie przetwarzania na uzasadnionym interesie administratora w kontekście licytacji na giełdzie reklam jest niewłaściwe**. Uzasadniony interes nie jest bowiem absolutny – administrator nie może się powołać na tę podstawę prawną w sytuacjach, „w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych". Biorąc pod uwagę potencjalny wpływ na prawa i wolności podmiotów danych, rozpowszechnianie danych osobowych użytkownika do szerokiego katalogu podmiotów trzecich, rodzące niewiadome skutki i pozbawione odpowiednich gwarancji nie może zostać uznane jako niezbędne do celów wynikających z prawnie uzasadnionych interesów.

c. Właściwą podstawą przetwarzania danych na rynku reklamy behawioralnej jest zgoda. Sposób zbierania zgody przez wiele portali internetowych jest jednak wątpliwy – często za wyraźną, potwierdzającą czynność zmierzającą do wyrażenia zgody uznawane jest zamknięcie okienka zawierającego informację o przetwarzaniu danych i przekazywaniu ich tzw. Zaufanym Partnerom, tj. setkom podmiotów uczestniczącym w licytacjach na giełdach reklam. Okienka te zostały zaprojektowane z wykorzystaniem tzw. *dark patterns*, czyli takich technik projektowania interfejsu, który skłania użytkownika do wyrażenia zgody. Przykładowo, aby zgodzić się na śledzenie i profilowanie przez setki podmiotów z branży reklamy behawioralnej wystarczy zamknąć okienko lub kliknąć duży, kolorowy przycisk „przejdź do serwisu". Aby nie wyrazić zgody, użytkownik musi wejść w „ustawienia zaawansowane", a następnie wybrać odpowiednie ustawienie prywatności, zamiast po prostu wybrać opcję „nie wyrażam zgody" na głównej planszy. **Naszym zdaniem taki sposób zbierania zgody jest niezgodny z RODO.**

d. W myśl art. 9 RODO, przetwarzanie danych szczególnie chronionych wymaga wyraźnej zgody (jeśli brak jest możliwości zastosowania innych przewidzianych w art. 9 podstaw prawnych). Tym niemniej, Standard IAB **umożliwia branży przetwarzanie danych wrażliwych bez zgody użytkownika**.

e. Wyraźna zgoda jest także wymagana do takiego przetwarzania, które skutkuje automatycznym podjęciem decyzji wobec jednostki. Jak wskazała Grupa Robocza Art. 29 w wytycznych w sprawie zautomatyzowanego podejmowania decyzji (WP251), przetwarzanie danych w celu wyświetlenia reklamy behawioralnej może mieć istotne skutki dla osoby, której dane dotyczą[10]. Skutki reklamy behawioralnej mogą być szczególnie dotkliwe np. w przypadku osoby, do której kierowana jest reklama usług, które mogą przynieść jej szkodę, np. usług hazardowych czy chwilówek. System nie przewiduje takiej możliwości, nie gwarantują też praw przewidzianych w art. 22 RODO.

[10] Np. biorąc pod uwagę głębokość profilowania, w tym śledzenie jednostek na różnych stronach, urządzeniach i w różnych usługach, oczekiwania jednostek czy wykorzystywanie wiedzy o słabościach osoby, której dane dotyczą.

f. Wyświetlanie użytkownikom spersonalizowanej reklamy wymaga wyróżnienia danego użytkownika na tle innych (tzw. koncepcja *single out*), w oparciu o identyfikatory związane z urządzeniem. Dostęp do tych identyfikatorów i ich odtworzenie przez użytkowników w celu zarządzania informacjami, które przechowują administratorzy, nie są proste. **Użytkownik nie zna tego numeru (każdy podmiot nadaje mu odrębny identyfikator, o którym użytkownik nie jest informowany), co uniemożliwia realizację uprawnień przewidzianych w RODO.** Konsekwencją jest poważna asymetria informacyjna pomiędzy użytkownikiem a podmiotami biorącymi udział w licytacjach na giełdach reklam.

g. Ta sytuacja jest elementem szerszego problemu bezpośrednio związanego z zasadą rzetelności i przejrzystości przewidzianą w RODO: **administratorzy danych mają prosty dostęp do identyfikatorów użytkowników, podczas gdy użytkownicy nie mają realnej możliwości kontrolowania lub wykorzystywania tych identyfikatorów**.

h. Na brak przejrzystości i nieprawidłowe informowanie użytkowników o przetwarzaniu danych w celu dopasowywania reklam w przypadku mobilnego systemu operacyjnego Android, którego właścicielem jest Google, zwrócił uwagę francuski organ ochrony danych osobowych w decyzji z 21 stycznia 2019 r., nakładając na Google karę w wysokości 50 mln euro[11].

28. *Ochrona danych w fazie projektowania i domyślne ustawienia prywatności (privacy by design i privacy by default)*

a. Jak wskazaliśmy powyżej, administratorzy danych mają prosty dostęp do danych użytkowników, podczas gdy użytkownicy nie mają realnej możliwości zweryfikowania, jak te dane są wykorzystywane. Kluczową trudnością jest samo zidentyfikowanie podmiotu, który przetwarza dane oraz identyfikatorów, którymi się posługuje. Nawet jeśli użytkownikowi uda się to ustalić podmioty biorące udział w licytacjach na giełdzie reklam bardzo często nie realizują one praw użytkowników, choćby prawa dostępu do danych, argumentując, że podanie internetowego identyfikatora nie wystarczy do zidentyfikowania konkretnej osoby. Praktyka pokazuje, że wiele firm z branży reklamy behawioralnej nie respektuje również ustawień „do not track", które użytkownik wybrał w przeglądarce. **Takie zaprojektowanie Systemu narusza art. 25 RODO,** który zobowiązuje administratorów do uwzględniania ochrony danych (w tym praw jednostek, które przewiduje RODO) już na etapie projektowania czynności przetwarzania i systemów, z których korzystają.

b. Warto zauważyć, że System IAB **powstał przed wejściem w życie RODO, kiedy w branży powszechny był pogląd, że identyfikatory internetowe i związane z nimi informacje nie stanowią danych osobowych**. W związku z tym, przy projektowaniu Systemu nie wzięto pod uwagę ochrony danych. Dostosowanie Systemu do nowego reżimu ochrony danych osobowych polegało nie na technicznym przeprojektowaniu systemu czy też zmianie sposobu jego

[11] https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

funkcjonowania, tam gdzie rodzi on ryzyko dla ochrony prywatności, ale **na takiej interpretacji przepisów – skądinąd wątpliwej – która zmierza do dopasowania już działających struktur technicznych do nowych ram prawnych**.

29. *Integralność i poufność*

    a. Standard IAB nie przewiduje odpowiedniej ochrony przed nieautoryzowanym i potencjalnie nieograniczonym ujawnianiem i przetwarzaniem danych osobowych.

    b. Standard IAB narusza przewidzianą w art. 5 ust. 1 lit. 7 RODO zasadę integralności i poufności danych, w szczególności poprzez:

        1. brak wymogu poinformowania podmiotów danych o rozpowszechnieniu ich danych lub o zamiarze rozpowszechnienia ich danych do każdego odbiorcy;
        2. brak przyznania użytkownikom możliwości zakomunikowania podmiotom trzecim swoich preferencji co do tego, w jaki sposób ich dane mogą być wykorzystywane;
        3. brak formalnego prawa sprzeciwu wobec wykorzystywania danych przez poszczególne podmioty trzecie;
        4. brak wystarczającej kontroli zmierzającej do zapobiegania nielegalnemu i/lub nieautoryzowanemu dalszemu wykorzystywaniu danych.

30. *Minimalizacja, prawidłowość i ograniczenie przechowywania*

    a. Liczba podmiotów, które otrzymują dane użytkownika, i brak realnych ograniczeń co do dalszego przetwarzania przez nie danych, rodzą poważne ryzyko wystąpienia negatywnych konsekwencji dla autonomii informacyjnej użytkowników.

31. *Ocena skutków dla ochrony danych*

    a. Biorąc pod uwagę szeroki zakres przetwarzanych danych oraz dużą liczbę podmiotów, które mają do nich dostęp, przetwarzanie danych na rynku reklamy behawioralnej może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W takich przypadkach art. 35 RODO wymaga przeprowadzenia oceny skutków przetwarzania dla ochrony danych. Z naszych informacji nie wynika, aby taka ocena została przeprowadzona lub udostępniona informacji publicznej.

VI. Podsumowanie

32. Funkcjonowanie Systemu rodzi poważne zagrożenia dla ochrony danych osobowych i autonomii informacyjnej użytkowników Internetu, w tym autonomii informacyjnej Skarżącej. Poszczególne podmioty na rynku reklamy behawioralnej współpracują

ze sobą i czerpią z tego finansowe korzyści, ale **za zagrożenia te odpowiedzialny jest przede wszystkim sam kształt Systemu stworzony przez IAB**.

33. Z tego powodu wnosimy do Prezesa Urzędu Ochrony Danych Osobowych jak we wstępie.
34. Jednocześnie deklarujemy gotowość do przekazania Prezesowi wyjaśnień i wszelkich dodatkowych informacji niezbędnych do podjęcia działań.

W imieniu Skarżącej

Małgorzata Szumańska

Wiceprezeska Fundacji Panoptykon

<u>Załączniki:</u>

Załącznik nr 1: Umocowanie

Załącznik nr 2: Odpis aktualny z KRS

Załącznik nr 3: Statut Fundacji Panoptykon

Załącznik nr 4: Treść skarg złożonych w Irlandii i Wielkiej Brytanii

Załącznik nr 5: Odpowiedź Prezesa UODO z dnia 10 stycznia 2019 r. na wystąpienie Fundacji Panoptykon w sprawie brokerów danych

Załącznik nr 6: Raport techniczny opisujący funkcjonowanie Systemów RTB